영국 정부, 사이버보안 역량 현황 보고서 발간

□ 개요

- 영국 디지털문화미디어스포츠부가 '20년 영국 노동 시장의 사이버보안 역량 현황을 조사한 보고서*를 발간(21.3.23.)

* Cyber security skills in the UK labour market 2021

□ 주요 내용

- **(인력 현황)** 전체 기업의 절반 가량(45%)이 한 명의 사이버보안 담당자를 두고 있으며, 보안 전문성도 부족한 것으로 나타남
 - 사이버보안 분야에서는 보안 인력의 49%가 해당 경력을 보유한 반면, 일반 기업에서 보안 업무를 겸직하는 직원의 86%는 과거에 다른 업무에 종사했던 것으로 조사됨
 - 대다수 기업(93%)이 사이버보안을 직원의 업무분장에 포함하지 않고 비공식적으로 처리하는 경향을 보임
- **(역량 격차)** 상당수의 영국 기업에서 사이버보안 관리에 필요한 기술 역량을 보유한 인력이 부족한 것으로 나타남
 - 전체 기업의 절반에서 개인정보 저장이나 이전, 방화벽 설정, 멀웨어 탐지 및 제거 등 기본 사이버보안 역량의 격차가 존재
 - 33%의 기업은 침투 테스트, 포렌식 분석, 보안 아키텍처 등 고급 역량에서, 32%는 사고 대응 역량에서 격차가 존재

- 사이버보안 분야에서는 전체 기업의 47%가 지난 12개월 간 사고관리와 조사, 디지털 포렌식 등의 영역에서 기술적 역량 격차를 겪었으며, 31%는 커뮤니케이션, 리더십 등 소프트 스킬 격차를 경험함
- **(자격과 훈련)** 사이버보안 분야에서는 일반 기업 대비 보안 기술 훈련이 보편적으로 실시되며 보안 자격증을 요구하는 경우가 많음
 - 사이버보안 기업의 79%는 지난 12개월 간 보안 담당 직원에게 훈련을 제공했다고 응답한 반면, 일반 기업에서는 해당 비율이 23%에 불과
 - 사이버보안 기업의 70%는 보안 관련 자격증을 보유하고 있거나 자격증 취득을 위해 일하고 있는 직원을 고용한다고 응답
 - 보안 인력 채용 시 가장 일반적으로 요구되는 자격증은 CISSP(Certified Information Systems Security Professional)이며, CCNP(Cisco Certified Network Professionals) 수요 또한 높음
- **(채용 현황)** 사이버보안 기업의 47%가 '19년 이후 보안 인력 채용을 실시했으며 이 중 37%는 결원을 채우는데 어려움을 겪음
 - 기업들은 채용이 어려운 원인으로 지원자의 기술적 역량이나 지식 부족(48%)을 주로 지적했으나, 자원자의 직무 경험 부족을 꼽은 비율도 35%에 달함
 - '20년 한 해 동안 사이버보안 직무 관련 온라인 채용공고 조사 결과 수요가 많은 일자리는 보안 엔지니어(34%), 보안 분석가(18%), 보안 관리자(14%), 보안 아키텍트(11%) 보안 컨설턴트(7%) 순임
 - 보안 인력을 가장 필요로 하는 산업군은 컨설팅, 금융과 보험, IT, 사이버보안 순으로 나타남

- 가장 수요가 많은 기술 역량은 네트워크 엔지니어링, 위협관리 및 기술적 제어, 운영시스템 및 가상화, 암호화, 프로그래밍 등임
- **(코로나19의 영향)** 코로나19 확산에 따른 이동제한 시행 중 사이버 보안 인력 채용이 일시적으로 감소했으나 '20년 하반기에는 이전 수준으로 회복됨
- 코로나19 기간 중 기업들이 급속히 원격근무로 전환하면서 사이버 보안이 전면으로 부각되어 보안부서의 업무가 가중된 한편, 교육과 인력 투자 확대의 기회도 마련됨
- 기업 및 채용기관들은 코로나19로 타격을 입은 산업군의 실직 증가로 일시적으로 사이버보안 인력풀이 늘어날 것으로 예상
- **(변화 추이)** '18년 조사결과와 비교해 사이버보안 역량 격차와 인력 부족 현상은 지속되었으나 일부 영역에서는 개선 추세
- 방화벽 구성, 소프트웨어 및 관리자 권한 제한, 보안 설정 및 패치 등의 영역에서 기본 역량의 격차를 드러낸 기업이 감소
- 기업 경영진이 조직 내 사이버 보안 위협을 이해하고 있다고 응답한 보안 책임자의 비율도 '18년 62%에서 '20년 77%로 증가
- 기술적 역량 격차가 존재한다고 응답한 사이버보안 기업들은 '18년 64%에서 '20년 47%로 감소
- **(권고사항)** 보고서는 조사결과를 바탕으로 사이버보안 역량 강화를 위한 태도·행동 변화, 경력 경로와 전환, 채용 및 인력 다양성 측면에서 권고사항을 제시

<사이버보안 역량 강화를 위한 권고사항>

영역	내용
태도·행동 변화	<ul style="list-style-type: none"> - 기업 경영진 차원의 사이버보안 위험 논의에 관해 국가사이버보안센터(NCSC)의 기존 지침*을 검토하고 필요시 업데이트하여 사이버 책임자가 상업적 위험 관점에서 사이버보안의 중요성을 강조할 수 있도록 지원 * NCSC 이사회 툴킷(NCSC Board Toolkit), 재택근무 지침(Guidance on home working) 등 - 사이버보안에 대한 기업 전반의 행동을 변화시키고 유지하기 위한 (인식 제고 및 교육 활동 등의) 지침 개발 및 관련 모범관행과 솔루션의 접근성 확대 - 공인 사이버 전문가 자격 요건에 조직 내 행동 및 문화에 긍정적인 영향을 미칠 수 있는 능력을 추가
경력 경로 및 전환	<ul style="list-style-type: none"> - 기업들이 보다 현실적인 채용 공고를 제시할 수 있도록 사이버보안 경력경로 안내 시 직무기술 예시 및 일반 직무에 대한 최소한의 자격 요건을 포함 - 사이버보안 경력경로 프레임워크 개발 시, 다양한 IT 인력이 사이버 전문가로 전환하거나 사이버보안 필수역량을 습득할 수 있는 교육 경로나 방법을 포함
채용 및 인력 다양성	<ul style="list-style-type: none"> - 사이버보안 분야의 중소기업이 전용 웹사이트나 인재교환 계획 등을 통해 학교들과 제휴관계를 체결해 인턴십 제도 등을 운영할 수 있도록 지원 - 중소기업의 사이버 책임자가 인력 다양성 제고를 위해 취할 수 있는 기본 행동을 안내하는 지침이나 교재 등을 개발 - 채용기관이나 인사팀이 사이버 책임자들에게 현실적이고 공정한 채용 모범 관행을 안내할 수 있는 워크샵 등의 행사 마련

□ 시사점

- 영국 정부의 이번 보고서에 따르면 상당수 기업이 기본적인 사이버 보안 역량 확보와 인력 채용에 어려움을 겪고 있으며, 이는 사이버 보안에 대한 경영진의 인식 부족에도 기인함
- 사이버보안 역량 강화를 위해서는 기업 전반의 사이버보안 인식 제고와 함께 제반 여건이 부족한 중소기업을 위한 인턴십 제도나 직무훈련 프로그램 지원 등의 방안 모색이 필요

[출처]

• Gov.uk, "Cyber security skills in the UK labour market 2021", 2021.3.23.